THE CHANGING FACE OF FRAUD:

2026 Identity Fraud Report

ENTRUST

Contents

ENTRUST

Foreword

Human perception has long been conditioned to trust what we see and hear – particularly when information comes from a source deemed credible. In today's AI-driven landscape however, that trust can no longer be taken for granted. Images, documents, videos, virtual meetings, and even phone calls can be synthetically generated or manipulated, challenging the very foundation of authenticity and reliability.

Over the course of my career speaking and engaging with the foremost innovators and technical leaders in the IT sector, the issue of identity protection remains a priority and even the most sophisticated organizations continue to confront this complex and evolving challenge.

In the cyber realm, trust and identity are inextricably linked – each dependent on the other. Without trust, identity cannot be verified; without verified identity, trust cannot exist. Today, that critical balance has been upended, as fraudsters around the world increasingly exploit advanced AI to manipulate and deceive.

In our ever-increasing digital reality, identity remains on the front line of defending against global fraud. The rapid adoption of AI across all platforms and arenas is enabling offenders to grow more cunning in their tactics and scale at levels and depths never seen before.

Fraud is becoming an enterprise unto itself with would-be fraudsters now gaining access to this cyber underbelly. No industry is immune to identity fraud, and the customer lifecycle is fraught with vulnerabilities, with variations across industries as to the most porous areas of threat. The playing field is evolving at break-neck speed, targeting people, their identities, plus the systems designed to protect it.

But just as AI is enabling the corrupt elements of the cyber world to propagate, it is also informing and empowering the good guys more readily and effectively to identify, meet, and neutralize the threats before they wreak havoc.

In my experience, only an effective, thoughtful, multi-tiered approach against identity fraud can stand up against the increasingly sophisticated tactics and tools employed by fraudsters. This report from Entrust provides a detailed analysis of the primary areas of vulnerability facing individuals and businesses today, and openly offers practical examples of the most common fraud vectors and effective strategies on how to prevent them.

Entrust's **"2026 Identity Fraud Report: The Changing Face of Fraud"** has its finger on the pulse and stands in a unique position to explore what's happening in the space, based on actual real-world experience and results.

Shira Rubinoff

CEO of The Cybersphere Group

Shira Rubinoff is a recognized cybersecurity executive, cybersecurity & AI advisor, global keynote speaker, analyst, author, and influencer, who has built two cybersecurity product companies, and led multiple women-in-technology efforts. She is currently the CEO of a cybersecurity consulting firm, The Cybersphere Group, and has served as a Chief Cybersecurity Officer and President and Founder of two cybersecurity product companies. Ms. Rubinoff also serves on advisory boards and provides guidance to numerous Fortune 100 companies in areas related to cybersecurity, AI, and company thought leadership. She consults various organizations in areas of business development and organizational dynamics.

Executive Summary

Fraud continues to rise in both scale and sophistication. Over the past year, we've seen attackers evolve rapidly – leveraging artificial intelligence (AI), automation, and organized fraud rings to exploit new vulnerabilities as defenses improve. Identity is now the front line of fraud, and protecting it requires a thorough understanding of tactics fraudsters leverage and how threat patterns are changing.

Fraudsters operate in three key ways:

1. **They target identity elements.**
   Fraudsters forge or steal identity documents, impersonate biometrics with deepfakes, or build entirely synthetic identities to bypass verification.
2. **They target prevention systems.**
   Injection attacks, device emulation, and automated bots aim to bypass verification flows and exploit the technology that's meant to stop them.
3. **They target people.**
   Psychological manipulation – from phishing and impersonation to coercion and romance scams – convinces victims to use their own genuine identity, hand over sensitive data, or transfer funds.

The data shows that fraud is becoming faster, more organized, and more commercially driven – a trend expected to continue through 2026. As generative AI (GenAI) and shared methodologies become more accessible, fraud attempts will likely increase in volume and sophistication, forcing organizations to strengthen defenses across every point of the identity lifecycle.

In this report, we'll explore how these threats are evolving, which industries are most affected, and where fraud is heading next. We'll also outline the prevention strategies that can help organizations build trust and stay ahead of emerging risks.

Report Methodology

This report draws on Entrust data from September 2024 through September 2025, covering:

1 billion+ identity verifications • 30+ industries • 195 countries

In some cases, data is compared to previous years to highlight year-over-year shifts and trends. While this report focuses on activity within the identity verification space – and may not always mirror wider market patterns – it represents one of the most comprehensive real-world views of how identity fraud is evolving.

Key Fraud Trends

ENTRUST

Fraud Snapshot

Across Entrust's global identity verification network, the average fraud rate in 2024 was 3.1%, up from previous years as attackers continue to evolve their methods and scale operations. Regional analysis shows significant variation:

At the same time, fraud tactics are shifting. As detection systems improve at stopping sophisticated threats like deepfakes, attackers are finding success by targeting the people behind the technology.

Social engineering is also up year-over-year and presents a concern in the identity space. Due to the nature of this type of fraud, it's tough to quantify. Still, coercion, phishing, and impersonation scams are harder to stop because victims are convinced – or forced – to use their own genuine identity credentials.

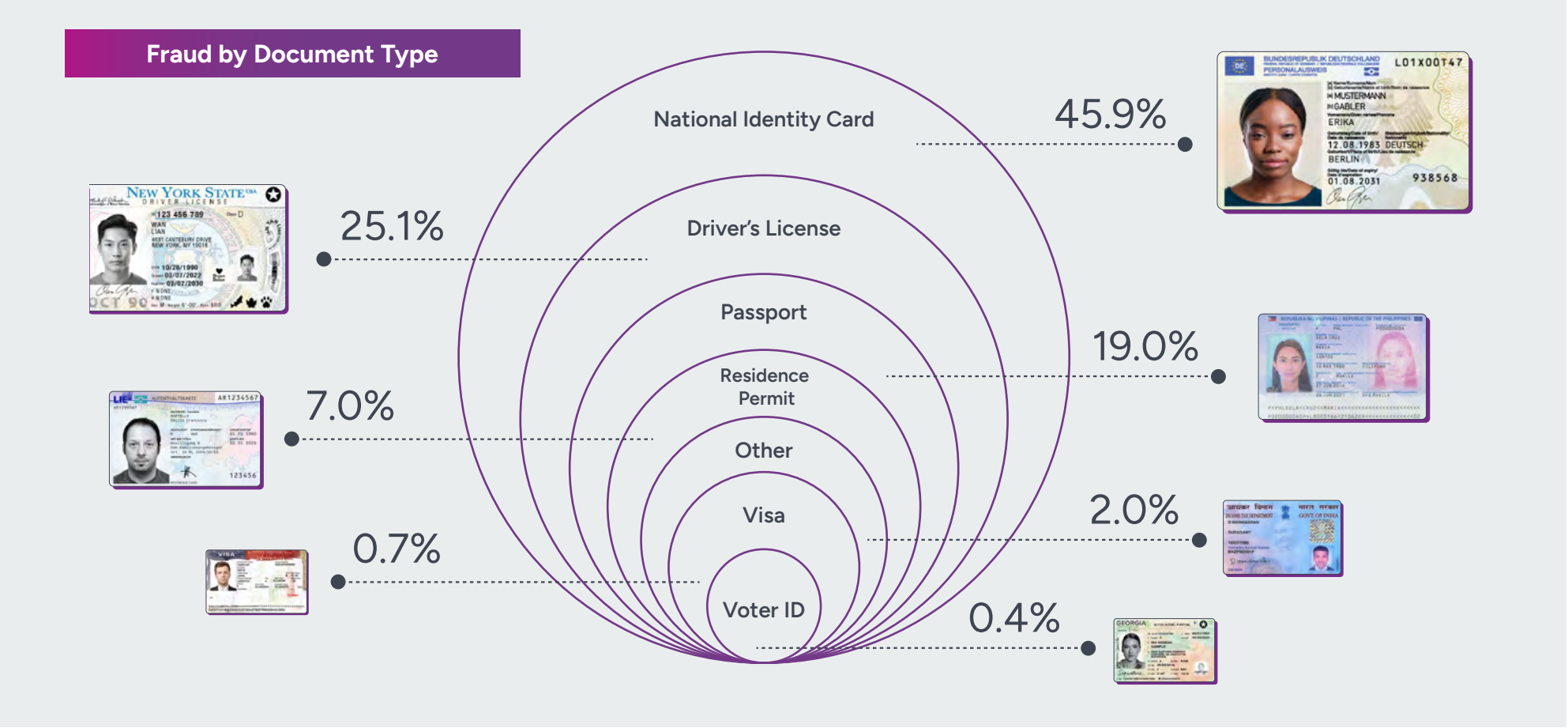
Fraudsters continue to use AI to help scale their attacks, with deepfakes now part of everyday life and linked to every 1 in 5 instances of biometric fraud.

Fraud patterns – specifically when fraud happens throughout the customer lifecycle, for example during onboarding or transactions – also vary by industry:

- **Crypto:** 67% of attacks occur at onboarding, often driven by sign-up bonuses.
- **Payments:** 82% of fraud attempts target the authentication process.
- **Digital Banks:** 55% of fraud happens after onboarding.

Document Fraud Remains an Established Part of Identity Fraud

Document fraud remains one of the most established and persistent forms of identity fraud. In 2025, national ID cards accounted for nearly half of all fraudulent document submissions globally (46%), followed by driver's licenses (25%) and passports (19%). Fraudulent national IDs are most prevalent in EMEA (45%) and APAC (60%), whereas AMER experiences more fraudulent driver's licenses (37%).



Top 10 Targeted Identity Documents

Not all national ID cards are designed for international travel (unlike passports), which means they don't need to adhere to International Civil Aviation Organization (ICAO) guidelines. Fraudsters often choose the path of least resistance, and with fewer security features and less robust guidelines, national ID cards remain an attractive route for fraudsters. Older, less secure versions of an ID card are likely to be in circulation. In other cases, even a more securely designed document may be targeted because it is the most used document in a region, or is seen as the least challenging alternative.

In 2025, bad actors targeted Bangladesh national ID cards more than any other document from any country. Many countries, such as Bangladesh and Pakistan, have older paper versions in circulation. These are thought to be more attractive for fraudsters, as they're easier to print at home.

Fraudsters also tend to take a "rinse and repeat" approach – recycling the same fake information across multiple fraudulent documents. Repeated names like Jon Doe, document numbers like A12345678, and birthdates, such as October 16, 1986, appear with suspicious frequency. These obvious fakes are easy to flag, but they serve as a distraction from more sophisticated fraudsters operating just behind them – the ones constantly refining their methods to stay undetected.

Document Fraud Goes Digital With GenAI

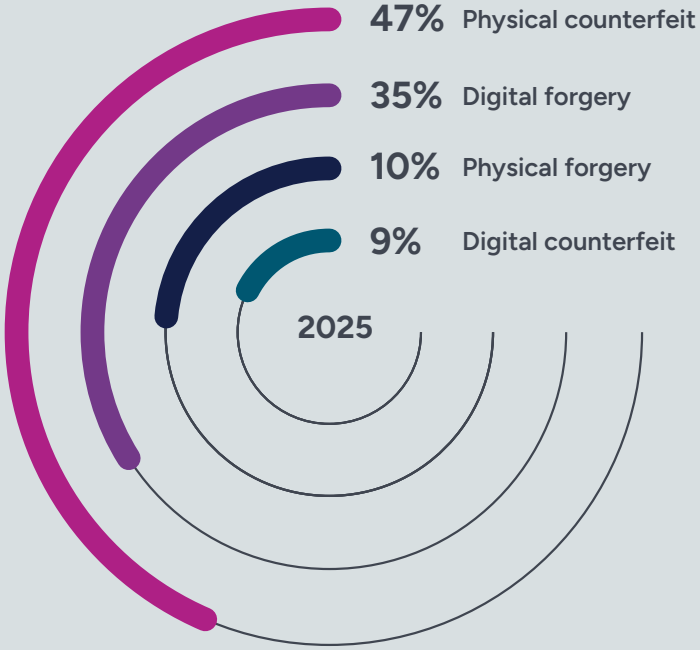
When defrauding identity documents, fraudsters use both counterfeits and forgeries, ranging from simple to highly sophisticated.

- **Counterfeits** are fabrications or reproductions of documents created from scratch and designed to look genuine. These can be created physically – such as printed or laminated fakes – or digitally, using tools that replicate official templates or add convincing security features.
- **Forgeries** involve altering an existing document (or image of a document), either physically (for example, swapping a photo or altering printed text) or digitally (editing an existing image of a document in Photoshop or another editing tool).

A few years ago, most attacks were physical counterfeits, and it was relatively uncommon to see digital manipulation techniques. But in recent years, there has been a shift toward digital attacks. In 2025, while physical counterfeits accounted for the majority of fraud attempts (47%), digital forgeries were also prevalent, accounting for 35% of attempts. The rise of digital methods is fueled by the accessibility and scalability of modern editing tools, which make it cheaper and faster for fraudsters to manipulate images, replicate templates, and mass-produce convincing forgeries.

GenAI has amplified this trend – enabling fraudsters to create hyper-realistic replicas of identity documents. What once required specialized software and design skills can now be achieved with an open-source model and a few prompts. While these AI-generated fakes can appear authentic to the human eye, they still leave detectable patterns that advanced machine-learning models can identify and block.

Macro Fraud by Type



What once required specialized software and design skills can now be achieved with an open-source model and a few prompts.

Deepfakes Account for 1 in 5 Biometric Fraud Attempts

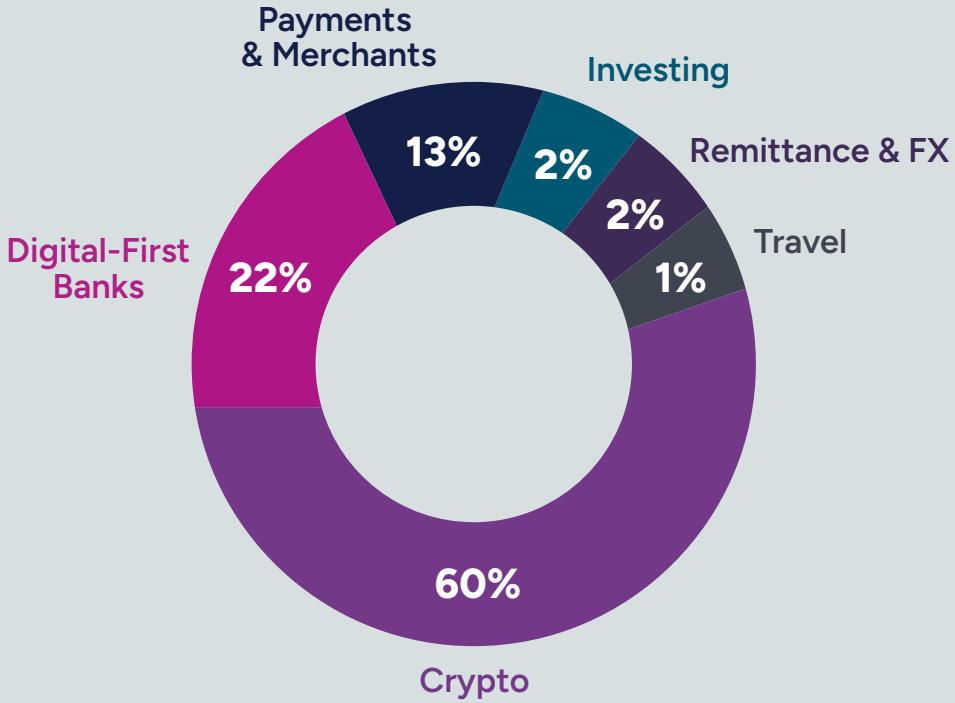
Deepfakes remain one of the most common biometric attack methods, with deepfakes being linked to approximately 1 in every 5 biometric fraud attempts.

Fraudsters use a wide range of deepfake methods, including:

- **Synthetic identities:** AI-generated faces that don't correspond to real people.
- **Face swaps:** Replacing one person's face with another in a recorded or live video.
- **Animated selfies:** Taking a static photo and using AI to add movement.

Presentation attacks make up the remaining distribution of biometric attack vectors. In these cases, fraudsters attempt to fool a biometric system using a fake object, for example by presenting a printed photo, a mask, or a video of a screen. These attempts are much easier to craft, making them a common first choice for fraudsters. However, modern biometric systems are designed to be robust against these simpler forms of spoofing, so attackers increasingly resort to AI-powered methods like the injection of deepfakes as the alternative way to attempt to bypass the system.

Deepfake attacks are especially prevalent in high-risk financial services:



How to Fight Biometric Fraud

As biometric fraud grows increasingly sophisticated, incorporating liveness detection and elements of randomness can offer enhanced protection against biometric attacks, including deepfakes and presentation attacks.

By introducing the requirement for liveness and irregular elements, systems can more effectively distinguish between genuine users and synthetic media. This approach makes it significantly harder for attackers to reuse static or pre-recorded content, which is often the case for deepfakes.

These advanced liveness checks help detect and deter a wide range of attempted biometric attacks, including:

- **Video of ID:** Recording or photographing the face printed on an identity document.
- **2D masks:** Flat, printed images worn or presented on camera.
- **3D masks:** Physical masks or objects designed to mimic a face.
- **Deepfakes:** Digitally altered photos or videos to impersonate someone.
- **Video on screen:** Recording a video that's already playing on a device.
- **Video of printout:** Filming an image that has been printed on paper.

At its core, liveness detection serves as a vital check ensuring that the submitted biometric data comes from an actual, living person, not from artificial representations.

Adding liveness – whether passive (detecting natural movement) or active (prompting specific actions) – provides temporal data that helps systems identify inconsistencies between genuine and fraudulent attempts. In Entrust's data, our active liveness solution, Motion Liveness, proves highly effective at preventing fraud, with a fraud rate of less than 0.1%.

Deepfakes

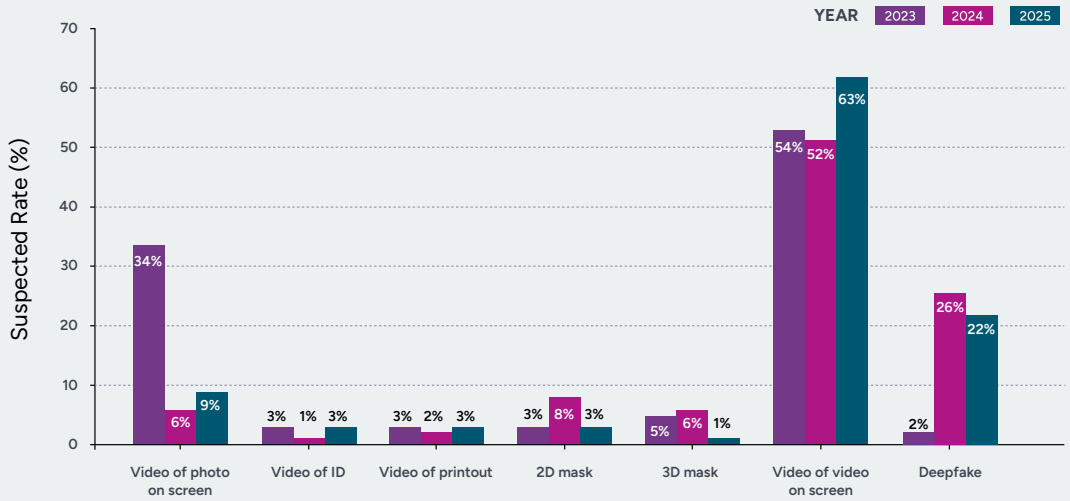
How to Fight Biometric Fraud

The nature of the product will have a difference on the types of attempted attacks observed:

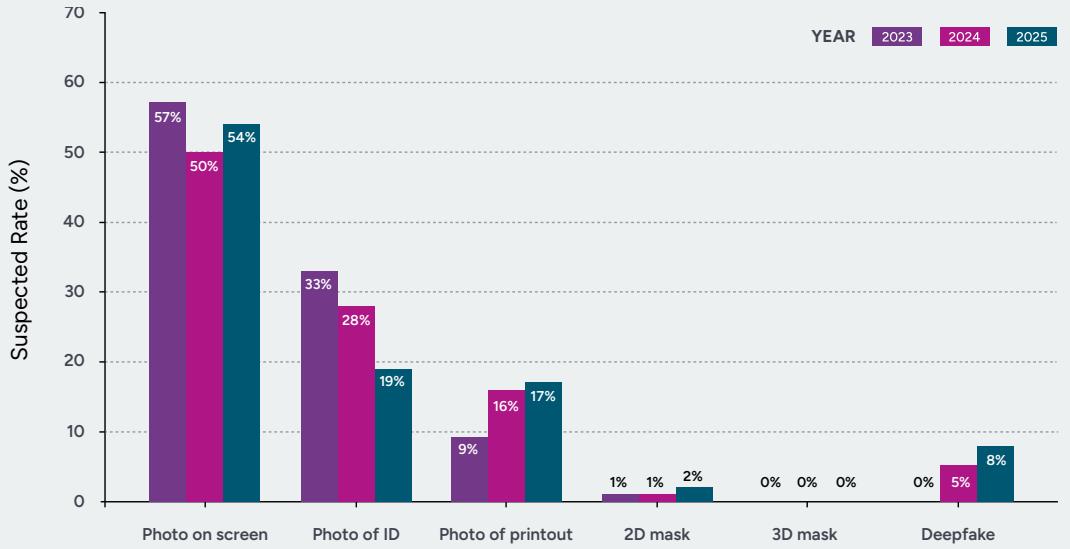
- **Across Selfie,** we see a higher proportion of low-tech attempts, such as photos on screens or ID printouts.
- **Across Motion Liveness,** attempted fraud tends to be more sophisticated, including deepfakes and real-time manipulation.

These trends reflect the evolving nature of attacks – demonstrating how fraudsters continuously keep testing verification systems using new methodologies, even when their attempts are blocked.

Fraud by Biometric Type - Motion



Fraud by Biometric Type - Selfie



The Rise of Injection Attacks

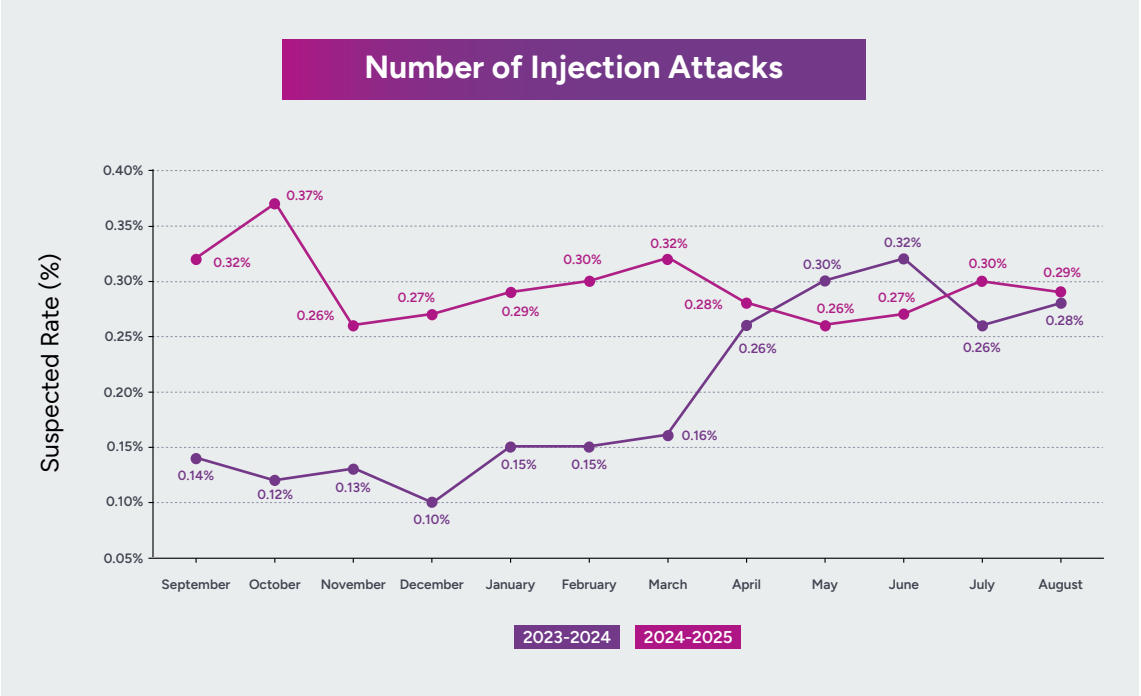
The main way fraudsters introduce sophisticated fraud such as deepfakes is through injection attacks. Falsified images or videos are fed directly into an identity verification system, bypassing the camera and live capture process entirely.

The cadence of injection attacks increased by roughly 40% year over year. These attacks are designed to manipulate verification systems at the technical layer rather than the user level. The main type of injection attack is via virtual camera injections, which are fake video streams presented to the verification system as if they were captured in real time.

Camera injection attacks are often paired with device emulation. Here a fraudster might first create an environment that looks like a standard, allowed device (such as the latest smartphone model), and then the virtual camera injection is used within that emulated environment to feed the fake video evidence to the verification software.

Fraudsters often use deepfakes combined with an injection attack to simulate a legitimate user, and without multi-layered fraud prevention solutions, they can be hard to detect. But there are proven countermeasures:

- **At the source (video input):** Using passive signals to check for suspicious activity or patterns linked to the media or device.
- **At presentation (video content):** Enforcing real-time biometric capture with dynamic interactions, or random cues.
- **At submission (back-end):** Analyzing the videos for anomalies or inconsistencies by cross-comparing inputs with AI model analysis systems to flag spoofs, for example deepfakes.



Automation and Device Emulation Scale With Fraud-as-a-Service

As verification technology advances, so do the tools fraudsters use to exploit it. Device emulation and automation have become key methods for scaling fraud, allowing attackers to mimic real user activity and overwhelm systems at volume.

Device emulation involves imitating a legitimate device's characteristics, such as its operating system or hardware signature, to make fraudulent activity appear authentic. Common examples include:

Digital Injection Attacks:
A fake video or image of a person's face or document is fed into a virtual camera within an emulated device, circumventing identity verification checks.

Multi-accounting:
Fraudsters create multiple accounts to exploit welcome bonuses and other incentives on platforms like online gaming or cryptocurrency exchanges.

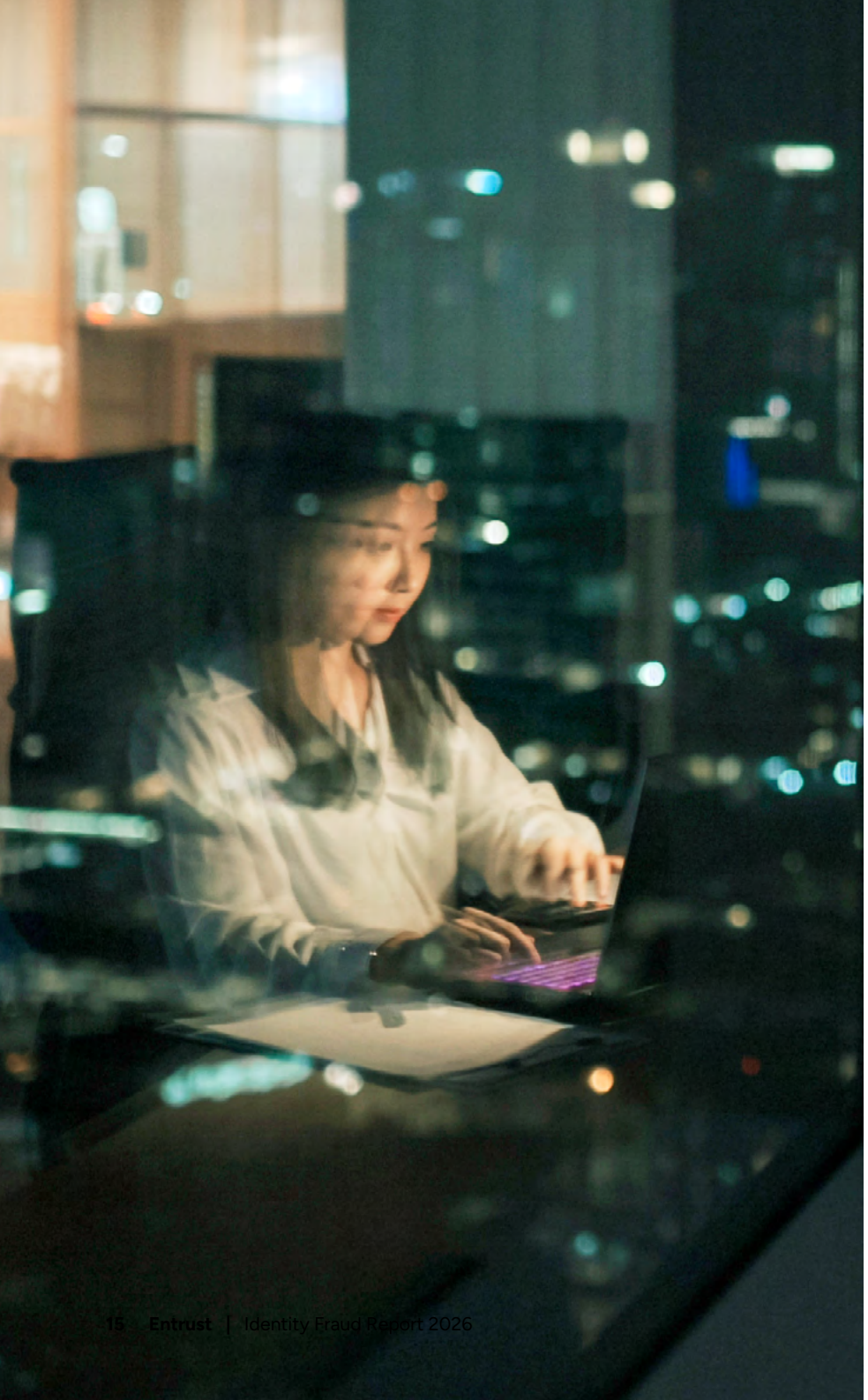
Account Takeovers (ATO):
Emulated devices can mimic legitimate user sessions to bypass security measures and gain access to user accounts.

Payment Fraud:
After gaining access to an account, fraudsters use emulated devices to conduct unauthorized transactions.

These capabilities are increasingly available through fraud-as-a-service platforms, which sell pre-built scripts, emulation tools, and credential lists to anyone willing to pay. This industrialization has lowered the barrier to entry for large-scale fraud.

It also highlights the importance of behavioral and device intelligence more than ever. Monitoring subtle signals from user environments, such as how devices report their capabilities and present themselves during verification, helps to detect inconsistencies that indicate emulation and spoofing.

New standards are also emerging in the industry, such as CEN/TS 18099, that aim to provide assurance around a vendor's ability to detect injection attacks. This reflects a growing recognition of how critical injection attacks are when it comes to verification, especially as they are the primary vector for introducing deepfakes into identity systems. Just as presentation attack detection (PAD) standards have helped to formalize defenses against spoofing, injection detection standards now offer a structured way to evaluate and mitigate these more advanced threats. It's a signal to the industry that injection attacks can no longer be overlooked.



How Fraudsters Manipulate Trust

Fraud prevention systems are stronger than ever, but people remain the most vulnerable link in the chain. In 2025, indicators suggest that social engineering and coercion pose an increasing threat to identity verification during the onboarding process.

Unlike technical fraud, these attacks manipulate victims into using their own real identity credentials. From phishing emails to romance scams and fake executives, fraudsters exploit human trust in ways that are extremely difficult for technology to block. Coercion attacks are uniquely difficult to detect because victims use their own genuine documents and biometrics – only under pressure or instruction from someone else.

The nature of this type of fraud is highly distressing and incredibly hard to quantify. Those most at risk are often vulnerable, and often it won't be apparent that a person has been coerced until suspicious activity emerges at a later stage.

To counter this, Entrust leverages checks to detect potential social engineering and also incorporates randomized motion prompts into biometric verification, making it harder for fraudsters to script or control the process.

The Professionalization of Fraud

Fraud today is no longer the work of isolated criminals – it's a global enterprise. Fraud rings are organized groups that plan and execute complex fraud operations, often spanning industries, regions, and platforms.

Entrust has identified 53 unique fraud rings since 2023, including four that have targeted multiple clients across different sectors. Fraud rings function much like legitimate companies. They have:

- **Defined roles:** Rings divide labor among recruiters, organizers, enforcers, and technical specialists.
- **Sophisticated operations:** Rings are capable of coordinating large, multi-step attacks.
- **Scale and specialization:** Rings range from small cells to hundreds of members, often focusing on a single fraud type such as credit card abuse or identity theft.

Their impact extends far beyond financial loss, damaging brand trust, regulatory standing, and customer confidence. Fraud rings thrive on weak spots, and they find them quickly. Businesses that lag in fraud prevention or cut corners on identity verification are often the first to be exploited.

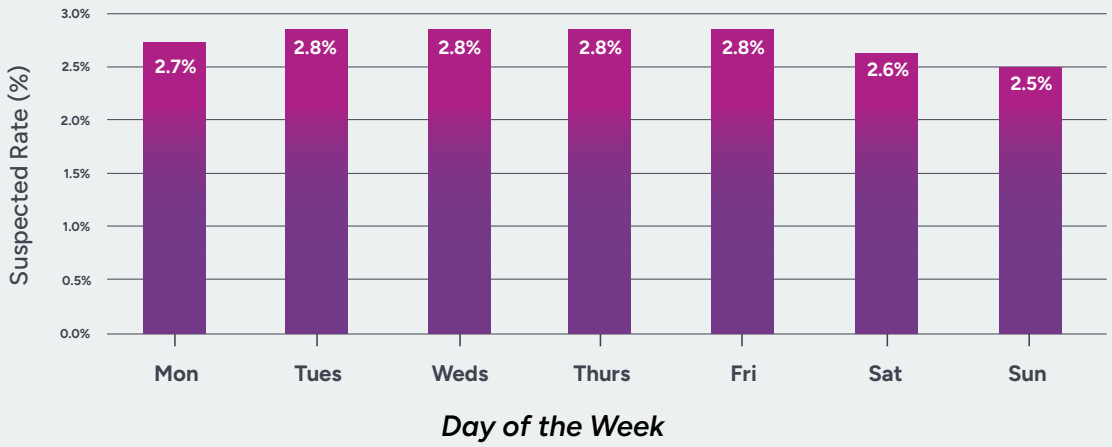
Fraud-as-a-Service Turns Fraud Into a Global Enterprise

Given the organized nature and scale of fraud operations today, it's no surprise fraud has become a 24/7 business. Organized fraud rings operate across continents and time zones, ensuring their attacks never stop. Entrust data shows that fraud attempts peak between 2 and 4 am UTC, when defenses in many regions are offline – illustrating how criminals coordinate globally to exploit gaps in coverage.

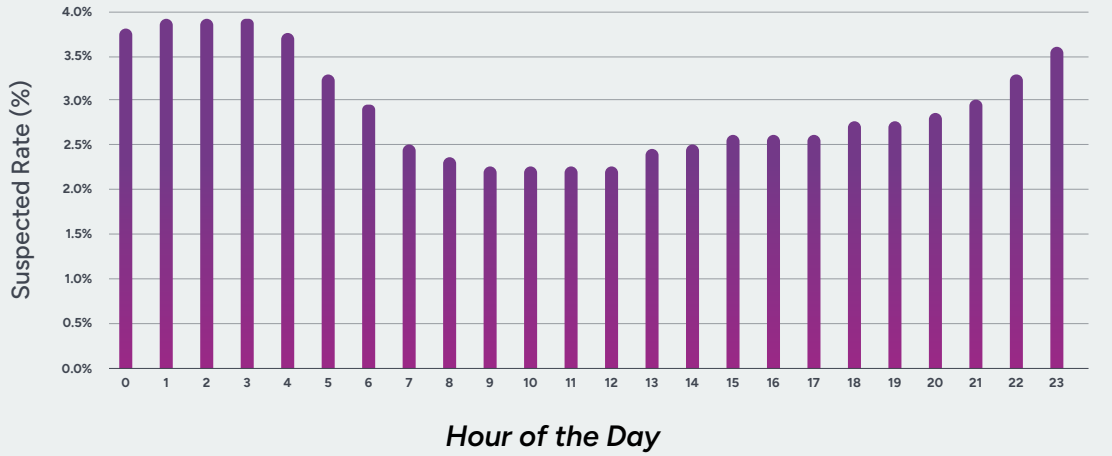
Modern fraud is also more accessible than ever. Attackers can now purchase ready-made kits, credential dumps, and AI-powered deepfake tools directly through encrypted messaging channels and dark web forums. These platforms have made professional-grade fraud available to anyone with minimal technical skill, fueling a surge in volume and sophistication.

The scale of fraudulent activities today highlights the importance of defenses that carry expertise across multiple geographies. By analyzing billions of verifications across 195 countries, Entrust identifies suspicious patterns that reveal fraud rings in action, linking cases through visual and non-visual signals, such as device or metadata anomalies.

Suspected Fraud Rate by Day and Hour



Fraud has become a 24/7 business. Entrust data shows that fraud attempts peak between 2 and 4 am UTC.



Industry Snapshots

ENTRUST

Fraudsters Set Their Sights on Crypto

Fraud rates in financial services vary widely – but none more so than crypto. Fraud activity in this sector has grown on average 24% every year since 2020, making it a constant pressure point.[1]

Cryptocurrencies are an attractive target for fraudsters because:

- They've soared in price and popularity in recent years.
- Their decentralized nature hinders asset recovery and transaction tracing.
- Many crypto platforms offer sign-up bonuses or rewards for significant deposits.

Cryptos are an especially prime target for scalable, AI-based attacks. They account for 60% of all deepfake fraud, while nearly 50% of document fraud attempts related to crypto companies are digital forgeries.

High-Value Transactions Face Heightened Risk

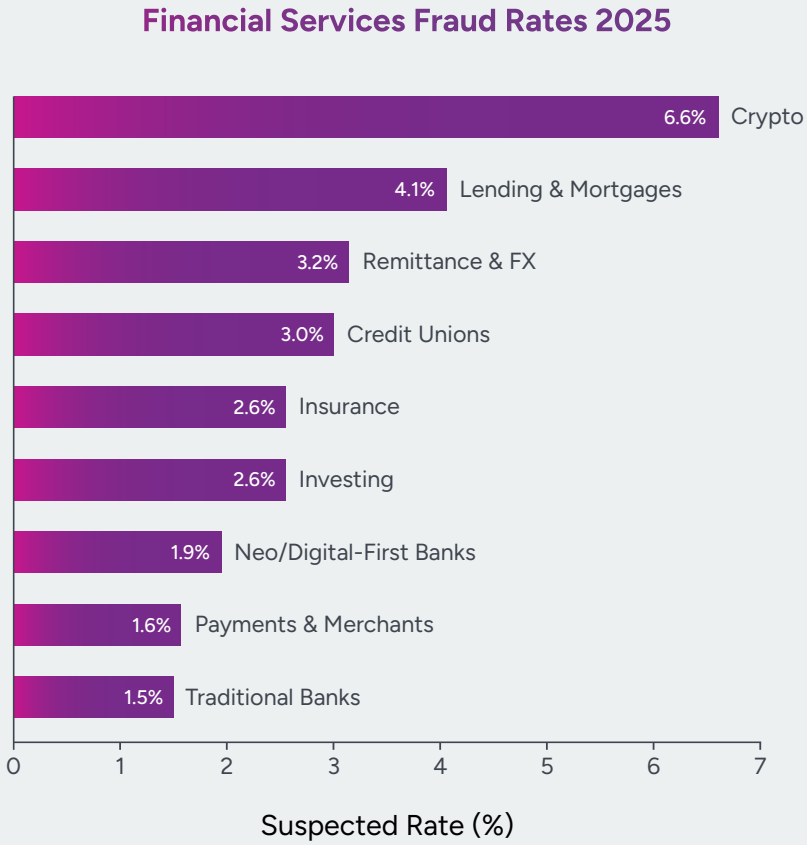
Beyond crypto, other areas of financial services are also experiencing rising fraud risk – particularly where high-value transactions or rapid digital onboarding are involved.

Lending and mortgages have seen a steady increase in fraud attempts, driven by economic pressure and rising interest rates. Fraudsters often use synthetic or stolen identities to apply for loans they have no intention of repaying, or to manipulate creditworthiness through falsified documents.

Remittance and foreign exchange (FX) services are frequent targets for money laundering and social engineering. Attackers exploit fast-moving, cross-border transactions to move or conceal illicit funds before detection systems can respond.

Other financial verticals – including insurance, credit unions, and digital-first banks – continue to face elevated exposure to both account takeover and new account fraud, especially as customer acquisition becomes increasingly digital.

While these threats vary by subsector, they share a common theme: Fraudsters follow opportunity. Wherever funds move quickly or verification is minimal, they will find ways to exploit it.



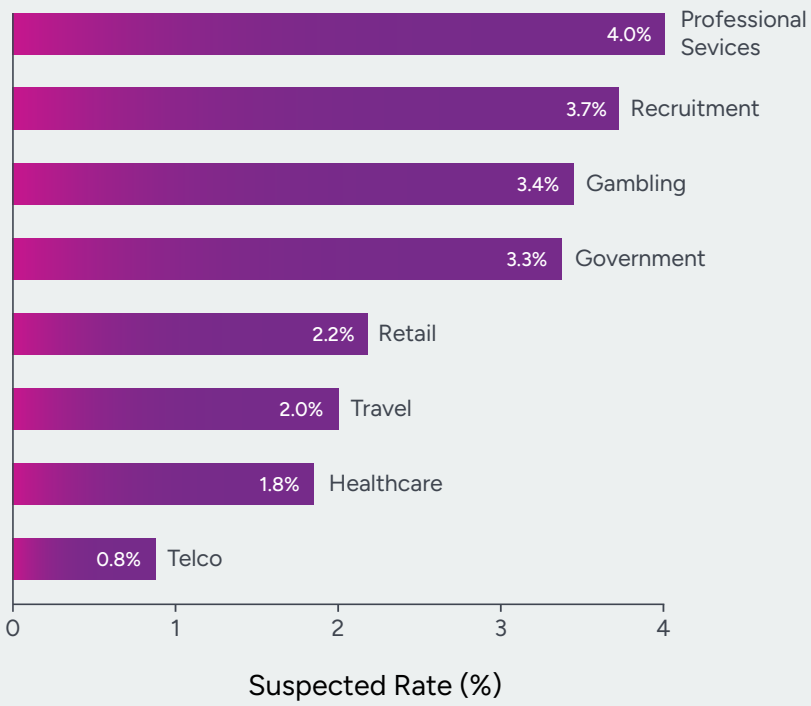
Lending and mortgages have seen a steady increase in fraud attempts, driven by economic pressure and rising interest rates.

Beyond Finance: Attempted Fraud Rates by Industry

Outside of financial services, identity fraud continues to affect a wide range of industries – particularly those that rely on remote onboarding, digital verification, or rapid user growth.

- **Professional services:** Law, consulting, and accounting, and other professional services firms are prime targets due to the combination of client data and high-value transactions. 44% of fraudulent documents submitted in this sector were passports, a favored form of ID in cross-border interactions.
- **Recruitment fraud:** Fake candidates are on the rise.[2] In fact, Gartner predicts that 1 in 4 job applicants will be fake by 2028.[3] Bad actors are using synthetic identities, deepfakes, and AI tools to apply for positions, infiltrating companies to steal data, plant malware, or steal funds. Fraudsters are now taking this further by combining hacked video links with deepfakes to conduct live, face-to-face interview scams. As remote work surges, businesses, recruiters, hiring managers, and job seekers must be cautious.
- **Gambling and gaming:** The main types of fraud that gaming and gambling companies see are multiple account creation, bonus abuse fraud, and money laundering. Recent regulatory introductions (such as the UK Online Safety Act) are also drivers for fraud in this sector. Since the Act introduced age restrictions in July 2025, there's been a surge in VPN usage as users attempt to bypass age verification.

Non-Financial Services Fraud Rates 2025



Upfront Incentives Drive New Account Fraud

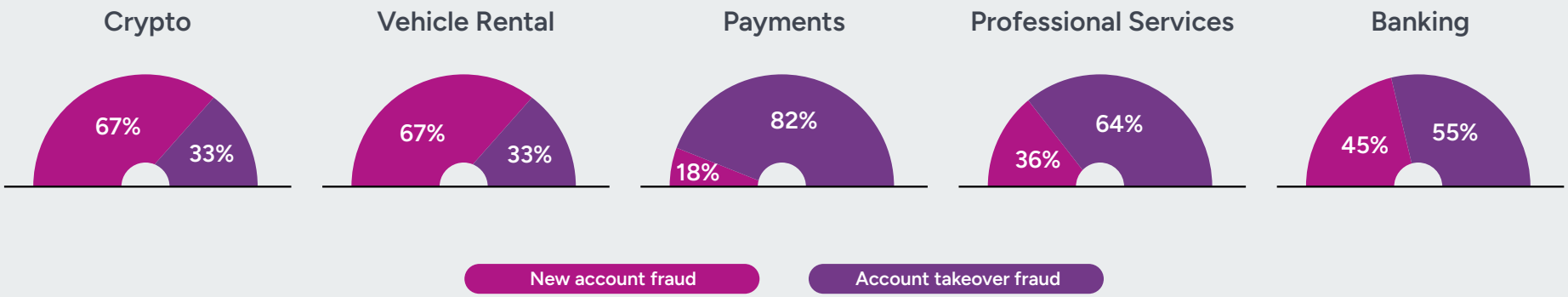
Fraudsters are opportunists. In industries where incentives or instant access are common, new account fraud dominates:

- **Crypto:** 67% of fraud attempts occur at onboarding, where sign-up bonuses attract large numbers of fraudulent applicants.
- **Vehicle rental:** Also 67%, as fraudsters use fake identities to gain temporary access to high-value assets.

Fraudsters exploit promotions, bonuses, or assets that can be quickly taken and moved. Overall, industries that offer incentives upfront are more likely to be targeted with new account fraud. On average, two-thirds of the fraudulent attempts they see are linked to new account fraud.

New Account Fraud Versus ATO Fraud

Overall, industries that offer incentives upfront are more likely to be targeted with new account fraud.



Account Takeovers Rise as Fraudsters Chase Long-Term Value

Once fraudsters gain access to a legitimate account, the potential damage multiplies. Account takeover fraud losses in the U.S. increased to $15.6 billion in 2024.[4]

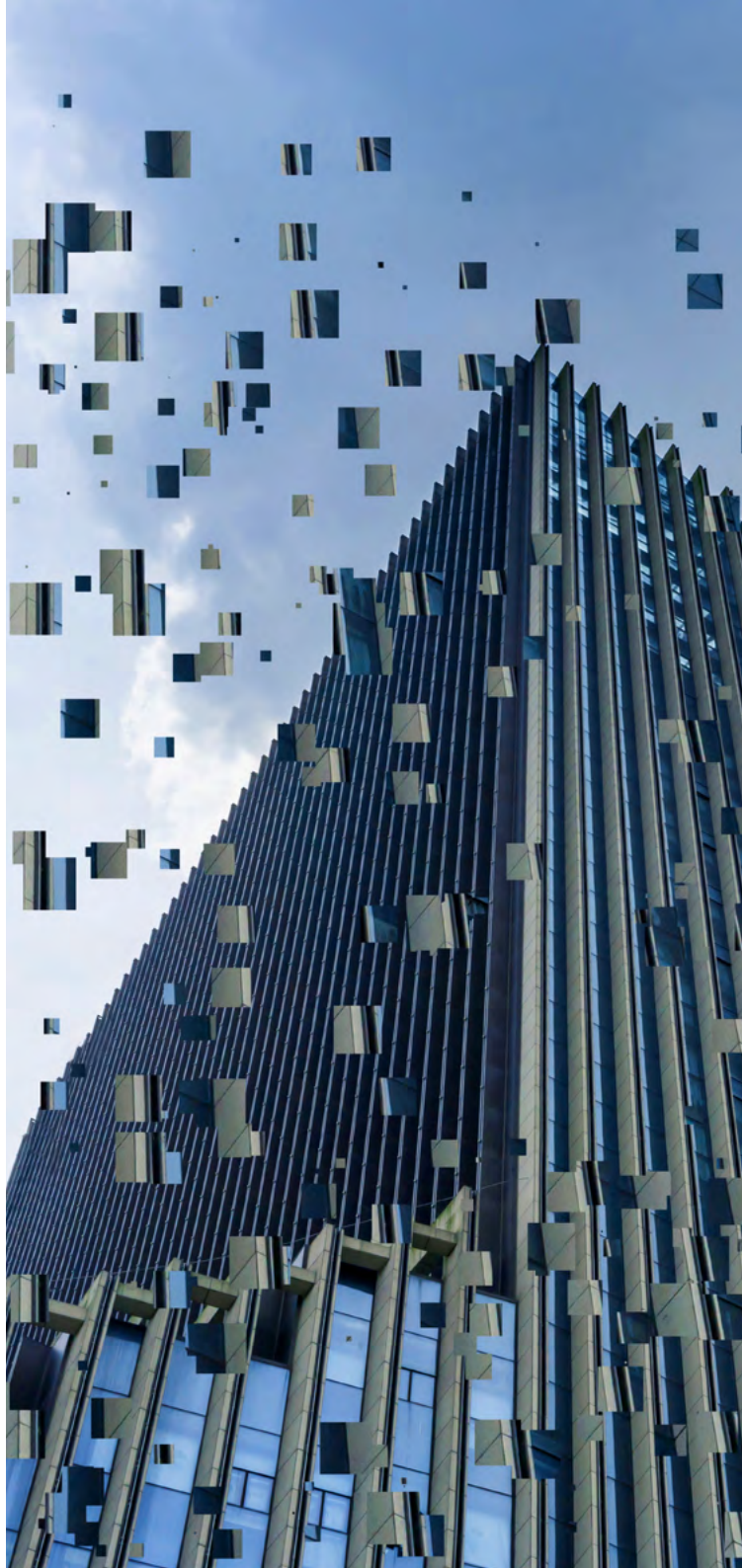
ATO fraud involves seizing control of an existing user account – typically through stolen credentials, phishing, malware, or social engineering – to steal funds, conduct unauthorized transactions, or harvest sensitive data.

Entrust data shows that ATO fraud is most common in industries where accounts hold long-term value:

Percentage of fraud that happens after onboarding

Payments	82%	Professional Services	64%	Digital-first Banks	55%

Fraudsters exploit these trusted accounts for loans, transfers, and identity-based data theft. On average, industries that offer long-term financial gain are twice as likely to experience ATO fraud.



Prevention

ENTRUST

Inside the Fraud Lab

The fraud prevention industry often relies on narrow datasets that don't reflect real-world conditions. Public sets like IDNet cover just a handful of attack types – a useful baseline – and offer a step in the right direction when it comes to benchmarking fraud prevention.

To more accurately reflect the types of fraud businesses experience on a day-to-day basis, we created an in-house Fraud Lab. Our dual approach combines:

- External datasets from labs and benchmarks, like IDNet, provide a common baseline.
- In-house fraud generation that simulates document and biometric attacks and more closely reflects what customers face on a day-to-day basis.

By narrowing the "domain gap" between synthetic samples and real-world fraud, we generate data that is more difficult for systems to detect – and better at predicting live performance.

Advice to Buyers

When evaluating fraud prevention vendors, it's not enough to ask, "What's your fraud performance?" Instead, ask the below questions as they reveal whether a vendor truly understands its system's strengths and limitations.

On what types of fraud samples was this measured?

How closely do these tests mirror real-world conditions?

Do you use adversarial testing (e.g., red teams) to probe weaknesses?

Can you show how false positives are distributed across regions or document types?

Are you transparent about failure cases – and why they occur?

Lifecycle Protection

Fraud isn't confined to a single moment – it can occur at any stage of the customer journey. Entrust enables organizations to build trust across the entire identity lifecycle, stopping fraud before it starts and helping to prevent it from resurfacing later.

- **Onboarding:** Document and biometric verification confirm users are who they claim to be before accounts are opened.
- **Authentication:** Multi-factor and biometric checks protect logins and re-verifications against account takeovers.
- **Transactions:** Device intelligence, anomaly detection, and behavioral signals safeguard high-risk activities like payments, transfers, or data access.

According to the 2025 Docusign and Entrust Future of Global Identity Verification report, organizations that implement robust identity verification save an average of $8 million per year in fraud-related costs.[5] Based on Entrust solution data, that equates to more than $5.5 billion in fraud losses prevented in 2025 – proof of the power of full-lifecycle protection.

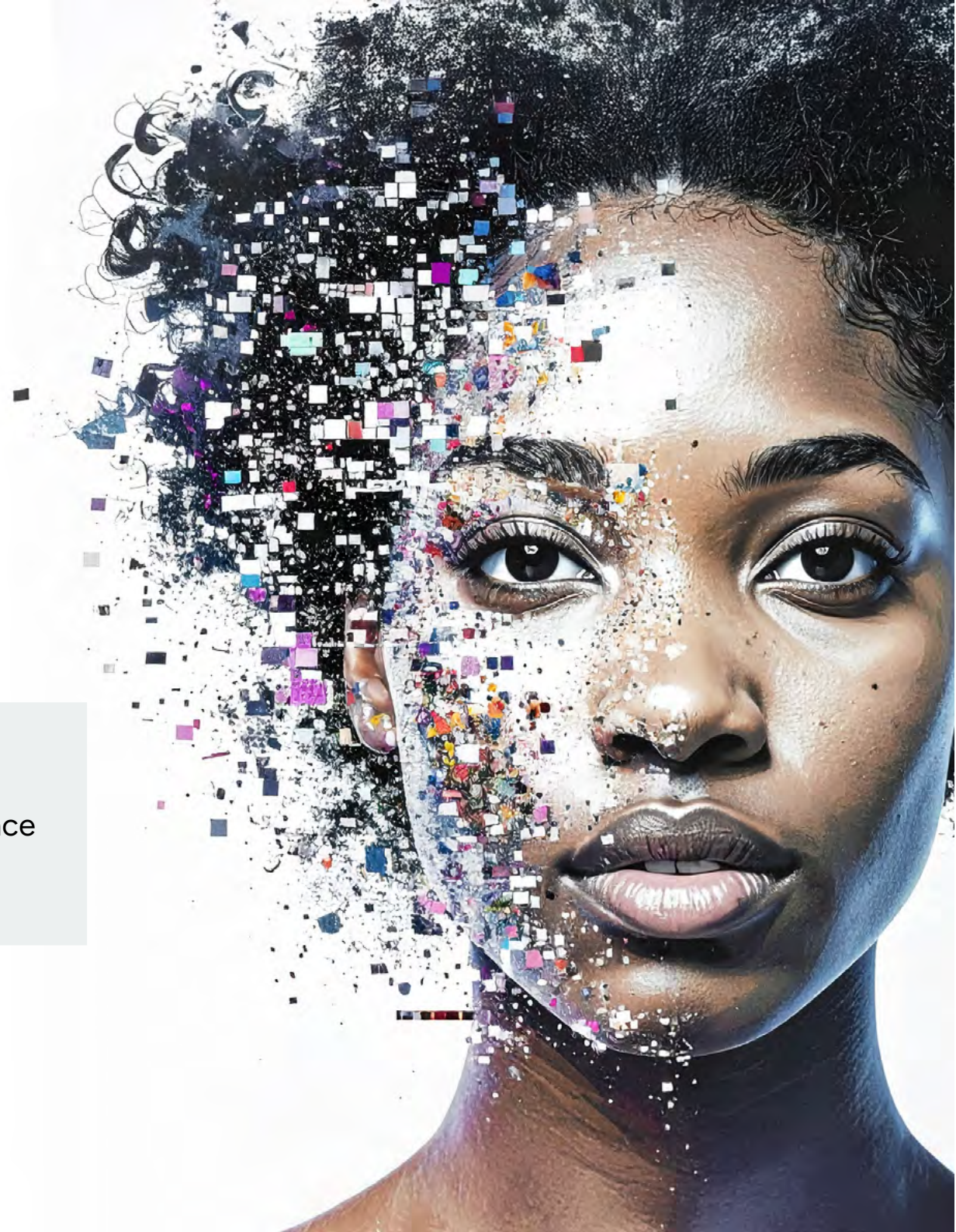
Prepare for the Future of Fraud

Fraud is evolving faster than ever – becoming more automated, organized, and industrialized. But as the threat landscape grows, so does the opportunity to stay ahead of it.

The future of fraud prevention lies in identity-centric, AI-driven defense. Organizations that protect every layer of identity – people, documents, biometrics, and systems – will be best equipped to adapt as fraudsters adopt new tools and tactics.

Entrust's global reach and deep fraud intelligence enable continuous innovation. With more than 1 billion identity verifications conducted across 195 countries and 30+ industries, Entrust delivers unmatched insight into how fraud operates – and how to stop it.

Secure every identity. Build trust everywhere. **Contact Entrust** and get ahead of the changing face of fraud now, tomorrow, and well into the future.



Fraud Attack Vectors Glossary

Fraud Risk	Examples	How to Prevent it
New account fraud Criminals use stolen, fake, or synthetic identities to open new accounts to gain illicit financial benefit.	• A fraudster uses a mix of fake and stolen information to open a bank account and apply for a credit card. • A fraudster uses fake information to take advantage of promotional bonuses offered by a gaming provider	Take a layered approach to defense to build a solid foundation of trust from day one. Combining document verification, biometric verification, trusted data sources, and signals.
Account takeover fraud (ATO) Fraudster gains unauthorized access to a legitimate user's account, such as a bank or e-commerce account, with the intention of stealing money, personal information, or selling the account to other criminals.	• Obtain login credentials through phishing, malware, or data breaches, and then use the compromised account to make fraudulent transactions, change personal details, or request new cards.	Tie users back to their trusted identity established at day one, with biometric authentication. Plus supplement with other auth methods like OTPs and passkeys.
Fraudulent documents Fraudulent documents are typically used as a way to open fake accounts. The ways criminals defraud documents include counterfeits (created from scratch) and forgeries (edits to existing documents). They tamper with either the real document or edit an image of a document in a digital setting.	• Physical counterfeit, where the fraudster has replicated an entirely new, fake document from scratch. • Digital forgeries, where a fraudster uses online tools like Photoshop to edit an existing image of a document (such as a sample photo of a document obtained via a data breach).	Document verification analyzes multiple factors, including data consistency across the document, visual features such as photos, and security features.
Deepfakes Deepfakes are realistic, AI-generated fake videos, images, or audio recordings that mimic a real person's likeness. Deepfakes pose a threat during both new account creation and authentication, as well as for social engineering attacks or investment scams.	• Fraudsters use a face swap (where a new face is superimposed onto a target head), combined with a stolen genuine ID, to open a fake account. These can be introduced via injection attacks or presentation attacks. • Fraudsters apply for jobs under a fake identity. • Imitating public figures or celebrities to endorse fake investments or other scams.	Biometric verification, powered by strong liveness detection and AI models that are resilient against next-generation deepfake creation tools, requires a secure live capture process. This process must include some element of motion and randomness and is essential for preventing pre-recorded content. For full assurance select vendors that are tested in compliance with ISO-30107 against presentation attack detection, across Level 1 and Level 2 attacks.

Fraud Attack Vectors Glossary

Injection attacks Fraudsters insert untrusted, malicious code or information into a system's input fields to bypass verification methods. It's one way fraudsters attempt to submit deepfakes or fraudulent documents.	A virtual camera to submit a deepfake or fraudulent document.	Preventing injection attacks requires a multi-layered approach, including leveraging passive signals, and a secure, real-time capture experience that assess elements of randomness. New standards are also emerging in the industry – such as CEN/TS 18099 – that aim to provide assurance around a vendor's ability to detect injection attacks.
Social engineering and coercion Attackers exploit human psychology and trust using manipulation, deception, or threats, rather than technical vulnerabilities. The aim is to gain unauthorized access to systems, data, or accounts through tactics like phishing, malware, or blackmail.	• Real-time coercion can be used to manipulate users into opening an account • Phishing attacks designed to trick people into handing over personal or account details. • Romance scams involving deepfake/impersonation fraud, designed to trick individuals into handing over money.	Social engineering and coercion can be incredibly hard to detect. However, a layered approach that combines trusted data sources, background signals to monitor for unusual behavior, and a verification process that includes an element of randomness make it harder for fraudsters to script or control the entire process.
Social Security number (SSN) fraud Fraudsters misuse a genuine Social Security number (SSN) for financial gain. Often, they will target children's SSNs, so the victim isn't aware until they come to use their SSN.	• Use SSNs to open new credit accounts in someone else's name.	Implement other forms of verification beyond just checking personal data, such as document and biometric verification.
Multi-accounts / bonus abuse fraud The same individual or group creates and uses multiple accounts to deceive or manipulate a system, often a platform like a betting site or crypto. This practice allows fraudsters to bypass restrictions, exploit system loopholes, and abuse incentives like sign-up bonuses.	• Fraudster creates multiple accounts to take advantage of a crypto platform's sign-up reward bonus.	Check for repeat information, including data (such as email addresses and phone numbers), as well as repeat document data, and the same faces appearing again (Known Faces).

Fraud Attack Vectors Glossary

Synthetic identity fraud Fraudsters create a fake identity by combining stolen, genuine personal information with invented details, like names, addresses, and Social Security numbers. Unlike traditional identity fraud, synthetic identities don't belong to a real person.	• Fraudster combines stolen SSNs with fake personal details to create a "Frankenstein" or synthetic identity to open an account and apply for credit.	Take a layered approach to defense, combining document verification, biometric verification, trusted data sources, and signals.
Credential stuffing A type of automated cyberattack where hackers take stolen username and password combinations, often obtained via a data breach, and use bot software to rapidly "stuff" the details into login forms to try and gain unauthorized access to accounts.	• Used as part of account takeover attempts to try and commit illicit transfers.	Monitor log-in attempts for suspicious activity using background signals (such as device and geolocation), as well as adopt biometric-based authentication.
Bot attacks Uses automated software programs, or "bots," to perform malicious actions at scale, such as credential stuffing to gain unauthorized account access.	• Automating credential stuffing to gain unauthorized access to accounts.	Monitor log-in attempts for suspicious activity using background signals (such as device and geolocation), as well as adopt biometric-based authentication.
Phishing Malicious attempts by criminals to deceive individuals into revealing sensitive information, such as login credentials, financial details, or personal data.	• Fake emails, texts, or calls impersonating a business or known contact.	Businesses should educate their users about the threats. Individuals should verify information, check sender details, and use strong security measures like MFA.
Money muling A type of money laundering where someone, called a "money mule," receives money from a third party and transfers it to another, often overseas. This process helps criminal organizations hide the origin of their illicit funds. The money mule may get recruited by fake advertisements or be coerced.	• Individuals transfer illegitimate or illegal funds overseas, for example, by exploiting gaps in verification.	Thorough KYC processes that include verifying customer identities, as well as monitoring for unusual behavior.

Sources

1. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/
2. https://www.cnbc.com/2025/07/11/how-deepfake-ai-job-applicants-are-stealing-remote-work.html
3. https://www.gartner.com/en/newsroom/press-releases/2025-07-31-gartner-survey-shows-just-26-percent-of-job-applicants-trust-ai-will-fairly-evaluate-them
4. https://javelinstrategy.com/research/2025-identity-fraud-study-breaking-barriers-innovation
5. https://go.entrust.com/docusign-future-global-identity-verification

About Entrust

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

entrust.com | Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST

SECURING A WORLD IN MOTION